DEPUTY SECRETARY OF DEFENSE

IO IO DEFENSE PENTAGON
WASHINGTON. DC 20301-1010

2 4 SEP 1998

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
CHIEFS OF SERVICES
DIRECTOR. DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST & EVALUATION
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANTS TO THE SECRETARY OF DEFENSE’
DIRECTOR. ADMINISTRATION AND MANAGEMENT
✓DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Information Vulnerability and the World Wide Web

The World Wide Web provides the Department of Defense with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies, and programs. It is at the heart of the Defense Reform Initiative and is key to the reengineering and streamlining of our business practices. Similarly, fundamental to the American democratic process is the right of our citizens to know what government is doing, and the correspondirg ability to judge its performance.

At the same time, however, the Web can also provide our adversaries with a potent instrument to obtain. correlate and evaluate an unprecedented volume of aggregated information regarding DoD capabilities. infrastructure, personnel and operational procedures. Such information, especially when combined with information from other sources, increases the vulnerability of DoD systems and may endanger DoD personnel and their families.

All DoD components that establish publicly accessible Web sires are responsible for ensuring that rhe information published on those sites does not compromise national security or place DoD personnel at risk. By authorizing the establishment of Web sites, component heads assume a management responsibility that extends beyond general public affairs considerations regarding the release of information into the realm of operational security and force protection. Component heads must enforce the application of comprehensive risk management procedures to ensure that the considerable mission benefits gained by using the Web are carefully balanced against the potential security and privacy risks created by having aggregated DoD information more readily accessible to a worldwide audicncc.

In view of the growing information role and vulnerability of the Web within DoD, I am directing the fallowing steps:

- Pending the development of detailed, procedural guidance, each component head shall immediately remove the following information from their publicly accessible (e.g. not password protected or domain restricted) Web sites.
  - Plans or lessons learned which would reveal sensitive military operations, exercises or vulnerabilities.
  - Reference to any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan of program.
  - All personal information in the following categories about U S. citizens, DoD employees and military personnel: 1) Social Security Account Numbers; 2) dates of birth; 3) home addresses, and 4) telephone numbers other than numbers of duty offices which are’appropriately made available to the general public. In addition, remove names. locations and any other identifying information about family members of DoD employees and military personnel.

    need to look ✓ at bios etc.

  - Addressees may grant waivers on a non-delegable basis when it has been determined that the immediate removal of information would adversely impact essential mission accomplishment.
- Within 60 days of the date of this memorandum, each addressee shall report the completion of the above actions to the Assistant Secretary of Defense Command, Control, Communications, and Intelligence (ASD(C3I)). Included in this report will be instances where-the addressee has granted a waiver.
  - During the above period, each component will evaluate the sensitivity of technological data included on its Web sites. These assessments will address the extent that such information, when compiled with other unclassified information, reveals an additional association or relationship that meets the standards for classification under Section 1.8 (e) E.O. 12958. Recommendations addressing this issue should be included in the above report.
- The Assistant Secretary of Defense (C3I) will establish a task force to develop policy and procedural guidance that addresses the operational, public affairs, acquisition, technology, privacy, legal, and security issues associated with the use of DoD Web sites. Preliminary guidance will be promulgated within 60 days from the date uf this memorandum
- Within 3 months of the promulgation of the above procedural guidance, addressees will ensure that a comprehensive, multi-disciplinary security assessment is conducted for their DoD Web sites, and annually thereafter.

- Within 6 *months* from the date of this memorandum, the Assistant Secretary of Defense (C3I) will develop, in coordination with the Chairman of the Joint Chiefs of Staff, USD (P&R), and OGC, recommendations relating to the establishment of a training program which addresses information security on the Web.

- Within 6 months from the date of this memorandum, the Assistant Secretary of Defense for Reserve Affairs and the Chairman of the Joint Chiefs of Staff will develop and implement a plan that uses Reserve Component assets to conduct ongoing operational security and threat assessments of component Web sites.

- The Assistant Secretary of Defense (C3I) will accelerate the development and implementation of an architecture which enhances the protection of Sensitive but unclassified information.

I believe that these steps will help us to manage Web information services better to strike the appropriate balance between openness and sound security. My point of contact is Mr. J. William Leonard. OASD(C3I) at (703) 697-2242.

John Hamre

John J. Hamre